IN THE CLAIMS

1. (currently amended) An information recorder ~~to~~ for recording information onto a recording medium, ~~the apparatus~~ said recorder comprising:

~~a~~ cryptography means ~~having a node key unique to each of nodes included in a hierarchical tree structure in which a plurality of different information recorders is included as each of leaves of the tree structure and a leaf key unique to each of the information recorders, and which encrypts data to be stored into the recording medium;the cryptography means~~ for generating an encryption key based on encryption key generating data built within ~~the~~ said information recorder ~~to~~ and for encrypting, using the generated encryption key, data that is to be stored ~~into~~ on the recording medium; and

memory means for storing a corresponding leaf key and at least a portion of a plurality of node keys, the plurality of node keys being associated with a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of nodes being arranged according to a hierarchical tree structure having a root node and having a specific leaf that is associated with said information recorder and with the corresponding leaf key, the portion of the plurality of node keys being the node keys associated with the nodes disposed along a path from the root node to the specific leaf,

the encryption key generating data being ~~data which can be~~ renewable~~ed~~ ~~with~~ using at least ~~either the~~ one of the corresponding leaf key and a selected one of the portion of the plurality of node keys,~~ or leaf key~~

the encryption key being a first encryption key and the encryption key generating data being first encryption key generating data when playback of the recording medium is to be restricted to only a player storing a specific identifier, the first encryption key generating data being stored on the recording medium, and

the encryption key being a second encryption key and the encryption key generating data being second encryption key generating data when playback of the recording medium is not to be restricted.

2. (original) The apparatus according to claim 1, wherein the encryption key generating data is a master key common to the plurality of information recorders.

3. (original) The apparatus according to claim 1, wherein the encryption key generating data is a medium key unique to a specific recording medium.

4. (original) The apparatus according to claim 1, wherein:

the node key can be renewed;

there is distributed, when a node key is renewed, a key renewal block (KRB) derived from encryption of the renewal node key with at least either a node key or leaf key on a lower stage of the tree structure to an information recorder at a leaf where the encryption key generating data has to be renewed; and

the cryptography means in the information recorder receives a renewal data for the encryption key generating data encrypted with the renewed node key, encrypts the key renewal block (KRB) to acquire the renewed node key, and calculates a renewal data for the encryption key generating data based on the renewed node key thus acquired.

5. (original) The apparatus according to claim 4, wherein:

the key renewal block (KRB) is stored in a recording medium; and the cryptography means encrypts the key renewal block (KRB) read from the recording medium.

6. (original) The apparatus according to claim 1, wherein:

the encryption key generating data has a generation number as renewal information correlated therewith; and

the cryptography means stores, as a recording generation number into the recording member, a generation number of the encryption key generating data having been used when storing encrypted data into the recording medium.

7. (cancelled)

8. (currently amended) The apparatus according to claim ~~7~~1, wherein~~ the cryptography means does as follows depending upon whether the player restriction is set or not~~:

when playback of the recording medium is not to be restricted~~the player restriction is not set~~, ~~the~~ said cryptography means generates a title-unique key from a master key, of which the generation is managed, stored in the information recorder, a disc ID being an identifier unique to a recording medium, a title key unique to data to be recorded to the recording medium and a device ID being an identifier for the information recorder to generate the first encryption key from the title-unique key; and

when playback of the recording medium is to be restricted to the player storing the specific identifier~~restriction is set~~, ~~the~~ said cryptography means generates a title-unique key from the generation-managed master key stored in the information recorder, disc ID being an identifier unique to the recording medium, title key unique to the data to be recorded to the recording medium and the device-unique key unique to the information recorder to generate the second encryption key from the title-unique key.

9. (original) The apparatus according to claim 1, further comprising a transport stream processing means for appending an arrival time stamp (ATS) to each of discrete transport packets included in a transport stream;

the cryptography means generating a block key as an encryption key for a block data including more than one packet each having the arrival time stamp (ATS) appended thereto; and

the cryptography means generating a block key as an encryption key, in encryption of the data to be stored into the recording medium, based on data including the encryption key generating data and a block seed being additional information unique to the block data including the arrival time stamp (ATS).

10. (original) The apparatus according to claim 1, wherein the cryptography means encrypts the data to be stored into the recording medium according to DES algorithm.

11. (currently amended) The apparatus according to claim 1, further comprising~~wherein~~:

~~there is provided~~ an interface means for receiving information to be recorded to a recording medium;

said ~~the~~ interface means identifying copy control information appended to each of packets included in a transport stream in a data to judge, based on the copy control information, whether or not recording to the recording medium is possible.

12. (currently amended) The apparatus according to claim 1, further comprising~~wherein~~:

~~there is provided~~ an interface means for receiving information to be recorded to a recording medium;

said ~~the~~ interface means identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the EMI, whether or not recording to the recording medium is possible.

13. (currently amended) An information player ~~to~~ for playing back information from a recording medium, ~~the apparatus holding~~ said information player comprising:

memory means for storing a corresponding leaf key and at least a portion of a plurality of node keys, ~~unique to each~~ the plurality of node keys being associated with a plurality of nodes ~~included in~~ whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of nodes being arranged according to a hierarchical tree structure ~~in which a plurality of different information recorders is included as each of leaves of the tree structure and a~~ having a root node and having a specific leaf that is associated with said information recorder and with the corresponding leaf key, the portion of the plurality of node keys being the node keys associated with the nodes disposed along a path from the root node to the specific leaf;~~unique to each of the information recorders, comprising a~~

cryptography means ~~to~~ for decrypting encrypted data stored in the recording medium~~; the cryptography means~~ using a decryption key and for generating ~~a~~ the decryption key based on decryption key generating data built in ~~the~~ said information recorder ~~to decrypt the encrypted data stored in the recording medium~~; and

the decryption key generating data being ~~data which can be~~ renew~~ed~~able ~~with~~ using at least one of the corresponding leaf key and ~~either the~~ a selected one of the portion of the plurality of node keys~~ or leaf key~~;

the decryption key being a first decryption key and the decryption key generating data being first decryption key generating data when playback of the recording medium is restricted such that said information player can play back information from the recording medium only if said information player stores a specific identifier, and

the decryption key being a second decryption key and the decryption key generating data being second decryption key generating data when playback of the recording medium is not restricted.

14. (original) The apparatus according to claim 13, wherein the decryption key generating data is a master key common to the plurality of information recorders.

15. (original) The apparatus according to claim 13, wherein the decryption key generating data is a medium key unique to a specific recording medium.

16. (original) The apparatus according to claim 13, wherein:

the node key can be renewed;

there is distributed, when a node key is renewed, a key renewal block (KRB) derived from encryption of the renewal node key with at least either a node key or leaf key on a lower stage of the tree structure to an information player at a leaf where the encryption key generating data has to be renewed; and

the cryptography means in the information recorder receives a renewal data for the decryption key generating data encrypted with the renewed node key, encrypts the key renewal block (KRB) to acquire the renewed node key, and calculates a renewal data for the decryption key generating data based on the renewed node key thus acquired.

17. (original) The apparatus according to claim 16, wherein:

the key renewal block (KRB) is stored in a recording medium; and

the cryptography means encrypts the key renewal block (KRB) read from the recording medium.

18. (original) The apparatus according to claim 13, wherein:

the decryption key generating data has a generation number as renewal information correlated therewith; and

the cryptography means reads, from the recording medium when decrypting encrypted data read from the recording medium, a generation number of the encryption key generating data having been used when encrypting the encrypted data and generates a decryption key from the decryption key generating data corresponding to the generation number thus read.

19. (cancelled)

20. (currently amended) The apparatus according to claim ~~19~~13, wherein~~ the cryptography means does as follows depending upon whether the player restriction is set or not~~:

when ~~the player restriction~~ playback of the recording medium is not restricted~~set~~, ~~the~~ said cryptography means acquires a generation-managed master key stored in the information recorder and acquires, from a recording medium, a disc ID being an identifier unique to a recording medium, a title key unique to data to be decrypted and a device ID being an identifier for the information recorder having recorded the encrypted data to generate a title-unique key from the master key, disc ID, title key and device key and the first decryption key from the title-unique key; and

when ~~the player restriction~~ playback of the recording medium is ~~set~~restricted and said information player stores the specific identifier, ~~the~~ said cryptography means acquires a generation-managed master key stored in the information recorder and a device-unique key unique to, and stored in, the information recorder and acquires, from a recording medium, a disc ID being an identifier unique to the recording medium and a title key unique to the data to be decrypted to generate a title-unique key from the master key, disc ID, title key and device-unique key, and the second decryption key is generated from the title-unique key.

21. (original) The apparatus according to claim 13, further comprising a transport stream processing means for controlling data outputting based on an arrival time stamp (ATS) appended to each of a plurality of transport packets included in the block data having been decrypted by the cryptography means;

the cryptography means generating a block key as a decryption key for a block data including more than one packets each having the arrival time stamp (ATS) appended thereto; and

the block key as a decryption being generated, in decryption of the encrypted data stored in the recording medium, based on data including the decryption key generating data and a block seed being additional information unique to the block data including the arrival time stamp (ATS).

22. (original) The apparatus according to claim 13, wherein the cryptography means decrypts the encrypted data stored in the recording medium according to DES algorithm.

23. (original)The apparatus according to claim 13, wherein there is further provided an interface means for receiving information to be recorded to a recording medium;

the interface means identifying copy control information appended to each of packets included in a transport stream in a data to judge, based on the copy control information, whether or not playback from the recording medium is possible.

24. (original) The apparatus according to claim 13, wherein there is further provided an interface means for receiving information to be recorded to a recording medium;

the interface means identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the

EMI, whether or not playback from the recording medium is possible.

25. (currently amended) An information recording method for recording information to a recording medium, ~~the~~ said method comprising ~~the steps of~~:

storing a corresponding leaf key and at least a portion of a plurality of node keys, the plurality of node keys being associated with a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of nodes being arranged according to a hierarchical tree structure having a root node and having a specific leaf that is associated with said information recorder and with the corresponding leaf key, the portion of the plurality of node keys being the node keys associated with the nodes disposed along a path from the root node to the specific leaf;

renewing encryption key generating data ~~to generate an encryption key for encrypting data to be stored into a recording medium with~~ built within an information recorder using at least ~~either~~ one of the corresponding leaf key and a selected one of the portion of the plurality of node keys ~~unique to each of nodes included in a hierarchical tree structure in which a plurality of different information recorders is included as each of leaves of the tree structure or a leaf key unique to each of the information recorders~~; ~~and~~

generating an encryption key based on the encryption key generating data; ~~to~~

encrypting, using the generated encryption key, data to be stored ~~into~~ on the recording medium;

the encryption key being a first encryption key and the encryption key generating data being first encryption key generating data when playback of the recording medium is to be restricted to only a player storing a specific identifier, the first encryption key generating data being stored on the recording medium, and

the encryption key being a second encryption key and the encryption key generating data being second encryption key generating data when playback of the recording medium is not to be restricted.

26. (original) The method according to claim 25, wherein the encryption key generating data is a master key common to the plurality of information recorders.

27. (original) The method according to claim 25, wherein the encryption key generating data is a medium key unique to a specific recording medium.

28. (currently amended) The method according to claim ~~15~~25, wherein:

the node key can be renewed;

there is distributed, when a node key is renewed, a key renewal block (KRB) derived from encryption of the renewal node key with at least either a node key or leaf key on a lower stage of the tree structure to an information recorder at a leaf where the encryption key generating data has to be renewed; and

the renewing step comprises steps of:

acquiring the renewed node key by encrypting the key renewal block (KRB); and

calculating a renewal data for the encryption key generating data based on the renewed node key thus acquired.

29. (original) The method according to claim 25, wherein:

the encryption key generating data has a generation number as renewal information correlated therewith; and the cryptography step further includes the step of storing, when storing encrypted data into the recording medium, a generation number of the encryption key generating data having been used, as a recording generation number into the recording medium.

30. (cancelled)

31. (currently amended) The method according to claim ~~30~~25, wherein~~ the cryptography means does as follows depending upon whether the player restriction is set or not~~:

when ~~the player restriction~~ playback of the recording medium is not restricted~~set~~, ~~the cryptography means~~ said generating step generates a title-unique key from a generation-managed master key stored in the information recorder, a disc ID being an identifier unique to a recording medium, a title key unique to data to be recorded to the recording medium and a device ID being an identifier for the information recorder and generates the first encryption key from the title-unique key; and

when ~~the player restriction~~ playback of the recording medium is ~~set~~restricted to an information player storing the specific identifier, said generating step ~~the cryptography means~~ generates a title-unique key from the generation-managed master key stored in the information recorder, disc ID being an identifier unique to the recording medium, title key unique to the data to be recorded to the recording medium and the device-unique key unique to the information recorder and generates the second encryption key from the title-unique key.

32. (original) The method according to claim 25, wherein there is further included a transport stream processing step of appending an arrival time stamp (ATS) to each of discrete transport packets included in a transport stream; in the cryptography step:

there is generated a block key as an encryption key for a block data including more than one packet each having the arrival time stamp (ATS) appended thereto; and

the block key as an encryption key is generated, in encryption of the data to be stored into the recording medium, based on data including the encryption key generating data and a block seed being additional information unique to the block data including the arrival time stamp (ATS).

33. (original) The method according to claim 25, wherein there is encrypted in the cryptography step the data to be stored into the recording medium according to DES algorithm.

34. (original) The method according to claim 25, wherein copy control information appended to each of packets included in a transport stream in a data is identified to judge, based on the copy control information, whether or not recording to the recording medium is possible.

35. (original) The method according to claim 25, wherein 2-bit EMI (encryption mode indicator) as copy control information is identified to judge, based on the EMI, whether or not recording to the recording medium is possible.

36. (currently amended) An information playback method ~~to~~ for playing back information from a recording medium, ~~the~~ said method comprising~~ the steps of~~:

storing a corresponding leaf key and at least a portion of a plurality of node keys, the plurality of node keys being associated with a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of nodes being arranged according to a hierarchical tree structure having a root node and having a specific leaf that is associated with said information recorder and with the corresponding leaf key, the portion of the plurality of node keys being the node keys associated with the nodes disposed along a path from the root node to the specific leaf;

renewing decryption key generating data ~~from which there is generated a decryption key for decryption of encrypted data stored in the recording medium with~~ built within an information player using at least ~~either~~ one of the corresponding leaf key and a selected one of the portion of the plurality of a node keys~~ unique to each of nodes included in a hierarchical tree structure in which a plurality of different information players is included as each of leaves of the tree structure or a leaf key unique to each of the information players~~; ~~and~~

generating the decryption key ~~from~~ based on the renewed decryption key generating data; ~~having renewed in the renewing step to~~ and

decrypting the data stored in the recording medium using the generated decryption key;

the decryption key being a first decryption key and the decryption key generating data being first decryption key generating data when playback of the recording medium is restricted such that the information player can play back information from the recording medium only if only the information player stores a specific identifier, and

the decryption key being a second decryption key and the decryption key generating data being second decryption key generating data when playback of the recording medium is not to be restricted.

37. (original) The method according to claim 36, wherein the decryption key generating data is a master key common to the plurality of information recorders.

38. (original) The method according to claim 36, wherein the decryption key generating data is a medium key unique to a specific recording medium.

39. (original) The method according to claim 36, wherein:

the node key can be renewed;

there is distributed, when a node key is renewed, a key renewal block (KRB) derived from encryption of the renewal node key with at least either a node key or leaf key on a lower stage of the tree structure to an information player at a leaf where the encryption key generating data has to be renewed; and

the cryptography step comprises the steps of:

encrypting the key renewal block (KRB) to acquire the renewed node key; and

calculating a renewal data for the decryption key generating data based on the renewed node key thus acquired.

40. (original) The method according to claim 36, wherein:

the decryption key generating data has a generation number as renewal information correlated therewith; and

in the cryptography step, there is read from the recording medium when decrypting encrypted data from the recording medium, a generation number of the encryption key generating data having been used when encrypting the encrypted data to generate a decryption key from decryption key generating data corresponding to the generation number thus read.

41. (cancelled)

42. (currently amended) The method according to claim ~~41~~36, wherein ~~the cryptography~~ said generating step includes ~~the following two procedures~~:

when playback of the recording medium is not to be restricted~~the player restriction is not set~~, ~~there is~~ acquiring~~ed~~ a generation-managed master key stored in the information player, ~~recorder and also~~ acquiring~~ed~~, from ~~a~~ the recording medium, a disc ID being an identifier unique to a recording medium, a title key unique to data to be decrypted and a device ID being an identifier for the information recorder having recorded the encrypted data to generate a title-unique key from the master key, disc ID, title key and device key and the first decryption key from the title-unique key; and

when playback of the recording medium is restricted and the information player stores the specific identifier~~restriction is set~~, ~~there is~~ acquiring~~ed~~ a generation-managed master key stored in the information ~~recorder~~ player and a device-unique key unique to, and stored in, the information ~~recorder~~ player, and acquiring~~ed~~, from a recording medium, a disc ID being an identifier unique to the recording medium and a title key unique to the data to be decrypted to generate a title-unique key from the master key, disc ID, title key and device-unique key; ~~and~~ the second decryption key being generated from the title-unique key thus generated.

43. (currently amended) The method according to claim 36, wherein:

the player includes a transport stream processing means for controlling data outputting based on an arrival time stamp (ATS) appended to each of a plurality of transport packets included in the decrypted block; and in the cryptography step:

a block key is generated as a decryption key for a block data including more than one packets each having the arrival time stamp (ATS) appended thereto; and the block key as a decryption is generated, in decryption of the encrypted data stored in the recording medium, based on data including the decryption key generating data and a block seed being additional information unique to the block data including the arrival time stamp (ATS).

44. (original) The method according to claim 36, wherein the encrypted data stored in the recording medium is decrypted according to DES algorithm.

45. (original) The method according to claim 36, wherein copy control information appended to each of packets included in a transport stream in a data is identified to judge, based on the copy control information, whether or not playback from the recording medium is possible.

46. (original) The method according to claim 36, wherein 2-bit EMI (encryption mode indicator) as copy control information is identified to judge, based on the EMI, whether or not playback from the recording medium is possible.

47.-56. (cancelled)

57. (currently amended) A ~~program serving~~ storage medium for ~~serving~~ storing a computer program ~~under which information processing~~ for carrying out a method of recording information to a recording medium~~ is conducted in a computer system~~, ~~the computer program~~ said method comprising~~ the steps of~~:

storing a corresponding leaf key and at least a portion of a plurality of node keys, the plurality of node keys being associated with a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of nodes being arranged according to a hierarchical tree structure having a root node and having a specific leaf that is associated with said information recorder and with the corresponding leaf key, the portion of the plurality of node keys being the node keys associated with the nodes disposed along a path from the root node to the specific leaf;

renewing encryption key generating data ~~to generate an encryption key for encrypting data to be stored into a recording medium with~~ built within an information recorder using at least ~~either~~ one of the corresponding leaf key and a selected one of the portion of the plurality of node keys ~~unique to each of nodes included in a hierarchical tree structure in which a plurality of different information recorders is included as each of leaves of the tree structure or a leaf key unique to each of the information recorders~~; ~~and~~

generating an encryption key based on the encryption key generating data; ~~to~~

encrypting, using the generated encryption key, data to be stored ~~into~~ on the recording medium;

the encryption key being a first encryption key and the encryption key generating data being first encryption key generating data when playback of the recording medium is to be restricted to only a player storing a specific identifier, the first encryption key generating data being stored on the recording medium, and

the encryption key being a second encryption key and the encryption key generating data being second encryption key generating data when playback of the recording medium is not to be restricted.

58. (currently amended) A ~~program serving~~ storage medium for ~~serving~~ storing a computer program ~~under which~~ for carrying out a method of playing back information stored in a recording medium ~~is played back in a computer system~~, ~~the computer program~~ said method comprising ~~the steps of~~:

storing a corresponding leaf key and at least a portion of a plurality of node keys, the plurality of node keys being associated with a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of nodes being arranged according to a hierarchical tree structure having a root node and having a specific leaf that is associated with said information recorder and with the corresponding leaf key, the portion of the plurality of node keys being the node keys associated with the nodes disposed along a path from the root node to the specific leaf;

renewing decryption key generating data ~~from which there is generated a decryption key for decryption of encrypted data stored in the recording medium with~~ built within an information player using at least ~~either~~ one of the corresponding leaf key and a selected one of the portion of the plurality of a node keys ~~unique to each of nodes included in a hierarchical tree structure in which a plurality of different information players is included as each of leaves of the tree structure or a leaf key unique to each of the information players~~; ~~and~~

generating the decryption key ~~from~~ based on the renewed decryption key generating data; ~~having renewed in the renewing step to~~ and

decrypting the data stored in the recording medium using the generated decryption key;

the decryption key being a first decryption key and the decryption key generating data being first decryption key generating data when playback of the recording medium is restricted such that the information player can play back information from the recording medium only if only an information player stores a specific identifier, and the decryption key being a second decryption key and the decryption key generating data being second decryption key generating data when playback of the recording medium is not to be restricted.